

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

SOCIALEDGE, INC. d/b/a CREATORIQ,

Plaintiff,

-v-

TRAACKR, INC. AND BEN STAVELEY,

Defendants.

23 Civ. 6860 (PAE)

OPINION & ORDER

PAUL A. ENGELMAYER, District Judge:

Plaintiff Socialedge, Inc., d/b/a CreatorIQ (“CreatorIQ”), alleges in this action that its former employee, defendant Ben Staveley, used his access to confidential and proprietary databases and information to funnel trade secrets to competitor and defendant Traackr, Inc. (“Traackr”), harming CreatorIQ’s business. *See* Dkt. 20 (“First Amended Complaint” or “FAC”). Pending before the Court is a motion by Traackr and Staveley to dismiss most claims in the FAC. Dkt. 25.

For the reasons that follow, the Court finds that, based on a stipulation entered during briefing, the motion is predominantly withdrawn. As to the surviving portion of the motion, which seeks dismissal of the FAC’s 11<sup>th</sup> claim, brought under the Computer Fraud and Abuse Act, (“CFAA”), 18 U.S.C. § 1030, the Court grants the motion and dismisses that claim.

## I. Background<sup>1</sup>

### A. Factual Background

CreatorIQ and Traackr are companies that help brands connect with social media “influencers” to launch and manage advertising campaigns. FAC ¶¶ 13–16. In or around November 2021, CreatorIQ acquired Tribe Dynamics, a marketing company also working in the social media space. *Id.* ¶¶ 18, 20. All employees of Tribe Dynamics became employees of CreatorIQ. These included Staveley, who became senior vice president for growth at CreatorIQ. *Id.* ¶¶ 21–22.

As part of his new role with CreatorIQ, the FAC alleges, Staveley had access to “highly confidential and proprietary product demonstrations, customer relationship management database . . . (which includes customer names and contacts), and customer-specific pricing information and product strategies.” *Id.* ¶ 22. CreatorIQ requires that executives and others with access to such information sign non-disclosure and confidentiality agreements. *Id.* ¶ 30. Consistent with that requirement, in October 2021, before becoming an employee of CreatorIQ, Staveley signed a “Confidential Information and Invention Assignment Agreement.” It required,

---

<sup>1</sup> The underlying facts which form the basis of this decision are drawn from the FAC. Dkt. 20. *See DiFolco v. MSNBC Cable LLC*, 622 F.3d 104, 111 (2d Cir. 2010) (“In considering a motion to dismiss for failure to state a claim pursuant to Rule 12(b)(6), a district court may consider the facts alleged in the complaint, documents attached to the complaint as exhibits, and documents incorporated by reference in the complaint.”). For the purpose of resolving a motion to dismiss under Rule 12(b)(6), the Court presumes all well-pled facts to be true and draws all reasonable inferences in favor of plaintiff. *See Koch v. Christie’s Int’l PLC*, 699 F.3d 141, 145 (2d Cir. 2012).

among other things, that he keep all “proprietary information confidential” and not retain any such confidential information upon termination of his employment. *Id.* ¶ 31.<sup>2</sup>

CreatorIQ takes other steps to protect its sensitive or proprietary information. These include requiring badges to access its corporate offices, implementing passwords and multifactor authentication to access its computers and/or “cloud-based applications,” and limiting access to certain information or functions to specific employees. *Id.* ¶¶ 37–39.

One customer relations database that CreatorIQ uses is Hubspot, Inc. (“Hubspot”). *Id.* ¶ 47. Only specified CreatorIQ employees or contractors are allowed to access CreatorIQ’s Hubspot accounts. *Id.* ¶¶ 49–50. During his employment at CreatorIQ, Staveley was one such employee. As such, he had administrator credentials associated with his work email address in order to access CreatorIQ’s Hubspot account. *Id.* ¶ 52.

In the three months leading up to his departure from CreatorIQ, Staveley used these credentials to export from Hubspot “more than 200,000 total records of CreatorIQ’s contacts and companies.” *Id.* ¶ 53. Separately, in or around January 2021, Staveley used his personal credentials to create a separate login ID (“SeedA Account”) connected to a personal email address of his: “ben@seedaconsulting.com.” *Id.* ¶ 54. “[P]ublicly available records [show that] SeedA Consulting Ltd. is a now-dissolved UK-based corporate entity which was created in or about January 2021 by Staveley.” *Id.* ¶ 55.

On or around October 2, 2022, approximately one year after becoming a CreatorIQ employee, Staveley gave notice of his planned resignation. *Id.* ¶ 43. On October 14, 2022, Staveley ended his employment with CreatorIQ. “Upon information and belief, Staveley

---

<sup>2</sup> Staveley appears to have signed this agreement with a Tribe Dynamics–affiliate, Tribe US, but it runs to “any of its current or future subsidiaries, affiliates, successors, or assigns” which includes CreatorIQ. FAC ¶¶ 31, 35.

immediately thereafter moved to New York City, and began working for Traackr from New York City.” *Id.* ¶ 45.

Despite no longer being an employee with CreatorIQ, Staveley, on 12 separate occasions between the time soon after he left CreatorIQ and August 9, 2023, used the SeedA account credentials he had created while at CreatorIQ to gain unauthorized access to a CreatorIQ-owned Hubspot account. *Id.* ¶ 56. Based on the IP addresses associated with these logins, all but one occurred in New York. *Id.* ¶ 58. Based on these unauthorized logins, CreatorIQ “hired a forensic expert to further investigate and conduct a damage assessment.” *Id.* ¶ 60.

In or around May 2023, a Traackr employee (“Jane Doe”) disclosed to a former CreatorIQ employee (“John Doe”) that Staveley had misappropriated CreatorIQ’s confidential and/or proprietary information, “including product demonstrations, customer lists, and contacts,” and shared it with Traackr and its employees during a “town hall” meeting he conducted. The FAC alleges, on information and belief, that this meeting took place in New York City. *Id.* ¶¶ 61–63. Jane Doe further disclosed that “Traackr specifically used the CreatorIQ confidential and proprietary information . . . to ascertain CreatorIQ’s perceived weaknesses . . . and to gain competitive intelligence with respect to one of CreatorIQ’s customers—one of the leading social media platforms in the world—for potential acquisition.” *Id.* ¶ 65.

The above misconduct, which the FAC alleges is ongoing, puts CreatorIQ in a position to “lose millions of dollars in business as well as the value of its goodwill, customer relationships, trade secrets, and confidential and proprietary information.” *Id.* ¶ 68. “Money alone,” the FAC alleges, “cannot make CreatorIQ whole.” *Id.* ¶ 73.

## II. Procedural History

On August 4, 2023, CreatorIQ filed the initial complaint. Dkt. 1. On August 21, 2023, Traackr and Staveley returned executed waivers of service. Dkts. 7–8. On October 17, 2023, Traackr and Staveley filed a motion to dismiss, Dkts. 12–13, after which the Court ordered CreatorIQ to either file an amended complaint or oppose to the motion, Dkt. 15. On November 7, 2023, CreatorIQ filed the FAC, the operative complaint today. It brings 11 claims:

1. for violation of the Defend Trade Secrets Act, 18 U.S.C. §§ 1836 *et seq.*, against Traackr and Staveley;
2. for violation of the California Uniform Trade Secrets Act (“CUTSA”), Calif. Civ. Code §§ 3426 *et seq.*, against Traackr and Staveley;
3. for common law misappropriation of trade secrets under both New York and California Law, against Traackr and Staveley;
4. for breach of fiduciary duty under New York and California law, against Staveley;
5. for breach of contract (without specifying the relevant state law), against Staveley;
6. for tortious interference with contract under New York and California law, against Traackr;
7. for violation of the California Business and Professions Code §§ 17200, *et seq.*, against Traackr and Staveley;
8. for unfair competition under both New York and California law, against Traackr and Staveley;
9. for unjust enrichment under New York and California law, against Traackr and Staveley;
10. for conversion under New York and California law, against Traackr and Staveley; and
11. for violation of the CFAA, 18 U.S.C. § 1030, as against Staveley.

FAC ¶¶ 74–185.

On November 21, 2023, defendants filed a joint motion under Rule 12(b)(6) to dismiss the FAC’s third, fourth, sixth, seventh, eighth, ninth, and 10<sup>th</sup> claims. Each brings a common law claim under both New York and California law. Dkt. 26 (“Def. Br.”) at 8. Defendants argued that California law applied to these claims, and that CUTSA thus preempted them. *Id.* at 5–11. Defendants also moved under Rule 12(b)(6) to dismiss the 11<sup>th</sup> claim, under the CFAA against Staveley. *Id.* at 12–13. Defendants’ motion did not challenge the FAC’s remaining claims, *i.e.*, its first, under the Defend Trade Secrets Act, against both defendants; its second, under CUTSA, against both defendants; or its fifth, for breach of contract, against Staveley. *See generally id.*

On December 12, 2023, CreatorIQ filed its opposition to dismissal. Dkt. 29 (“Pl. Br.”). Among its arguments, CreatorIQ argued that New York, not California, law applies to its common law claims, and that CUTSA, a California statute, cannot preempt claims under New York law. *Id.* at 8–16. CreatorIQ stated that, “to prove this point, CreatorIQ is willing to withdraw its California law-based causes of action if the parties stipulate that New York law applies to all of CreatorIQ’s causes of action, except for its breach-of-contract claim.”<sup>3</sup> *Id.* at 16 n.1.

On December 22, 2023, the defendants filed a reply. Dkt. 30 (“Def. Reply”). Relevant here, it stated that “[w]hile Defendants cannot agree that the facts alleged in Plaintiff’s Amended Complaint support the application of New York law, Defendants will stipulate to the application

---

<sup>3</sup> Explaining that exclusion, defendants state that the contract underlying that claim has a provision making California law applicable to it. Def. Reply. at 1.

of New York law in order to move this case forward[.]” *Id.* at 1. Defendants thus limited their reply to addressing the FAC’s 11th claim, under the CFAA. *Id.* at 2.

### III. Discussion

#### A. The Parties’ Mid-Litigation Stipulation

At the threshold, the Court considers what it treats—based on statements in the sequence of briefs—as a joint stipulation that plaintiff will withdraw any California common law claims if defendants stipulate that New York law applies to these claims, and that defendants accordingly will withdraw their motion to dismiss these counts, which is based solely on the argument that these are preempted by a California statute, CUTSA. *See* Pl. Br. at 16 n.1; Def. Reply at 1–2. For the following reason, the Court will give effect to this stipulation, which greatly narrows the scope of the pending motion to dismiss.

Whether to approve the stipulation requires the Court first to determine which state’s law governs the issue. In exercising supplemental jurisdiction over the FAC’s common-law claims,<sup>4</sup> the Court applies the choice of law rules of the forum state—New York—to decide questions relating to such claims. *Rogers v. Grimaldi*, 875 F.2d 994, 1002 (2d Cir. 1989) (“A federal court . . . adjudicating state law claims that are pendent to a federal claim must apply the choice of law rules of the forum state.”). And courts applying New York choice-of-law rules have held that “in the absence of strong countervailing public policy, the parties to litigation may consent by their conduct to the law to be applied.” *Walter E. Heller & Co. v. Video Innovations, Inc.*, 730 F.2d 50, 52 (2d Cir. 1984) (citing *Martin v. City of Cohoes*, 371 N.Y.S.2d 687, 690 (1975));

---

<sup>4</sup> This court has subject matter jurisdiction over CreatorIQ’s federal-law claims under the Defend Trade Secrets Act (the “DTSA”), 18 U.S.C. § 1836, and CFAA. *See* 28 U.S.C. § 1331. It thus has supplemental jurisdiction over the remaining state law claims pursuant to 28 U.S.C. § 1367.

*Trophy Prods., Inc. v. Cinema-Vue Corp.*, 385 N.Y.S.2d 70, 73 (1976); *El Hoss Eng'g & Transp. Co. v. Am. Indep. Oil Co.*, 183 F. Supp. 394, 399–400 (S.D.N.Y. 1960), *rev'd on other grounds*, 289 F.2d 346 (2d Cir.), *cert. denied*, 368 U.S. 837 (1961)). Consistent with this, courts in this Circuit have honored parties' agreements as to the applicable law, including when reached in mid-litigation and when implicit as opposed to formalized. *See, e.g., Tehran-Berkeley Civil and Env'l Eng'rs v. Tippetts-Abbett-McCarty-Stratton*, 888 F.2d 239, 242 (2d Cir. 1989) (applying New York law where parties relied on New York law in briefs); *Larsen v. A.C. Carpenter, Inc.*, 620 F. Supp. 1084, 1103 (E.D.N.Y. 1985), *aff'd*, 800 F.2d 1128 (2d Cir. 1986) (finding that forum law governed, given parties' implied stipulation to the same, notwithstanding arguments that foreign law might otherwise apply); *Geller v. Delta Air Lines, Inc.*, 717 F. Supp. 213, 214–15 (S.D.N.Y. 1989) (honoring stipulation at pre-trial conference as to choice of law).<sup>5</sup>

The Court is unaware of any “strong countervailing public policy” to applying the law of forum-state New York to this controversy. The Court hence accepts the parties' stipulation. And there is a sound factual basis on which to apply New York law: the FAC alleges that both CreatorIQ and Traackr have offices and do business in New York, that some alleged misconduct occurred via unauthorized logins in New York, and that Staveley resides (and may still reside) in New York. FAC ¶¶ 45–63; *see also* Def. Br. at 9–11 (not disputing latter point).

---

<sup>5</sup> Agreements as to the applicable law in the event of a dispute are often in contracts that predate the dispute being litigated. Courts accept these provisions “as long as the jurisdiction chosen has a substantial relationship to the parties . . . and the fundamental policies of New York law are not violated.” *See Yankee Caithness Joint Venture, LP v. Planet Ins. Co.*, No. 94 CIV. 8939, 1996 WL 426359, at \*2 (S.D.N.Y. July 30, 1996) (citing *Woodling v. Garrett Corp.*, 813 F.2d 543, 551 (2d Cir. 1987)). Relevant here, courts have also overwhelmingly honored mid-litigation agreements as to the governing law. *Hamilton v. Accu-Tek*, 47 F. Supp. 2d 330, 343 (E.D.N.Y. 1999).



The Court thus treats all of the FAC's common law claims as arising under New York law only. The Court accordingly treats defendants' motion to dismiss based on the preemption of common law claims by CUTSA as withdrawn.

### **B. Motion to Dismiss CFAA Claim**

The Court next considers the motion to dismiss the FAC's CFAA claim. To survive a motion to dismiss under Rule 12(b)(6), a complaint must plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A complaint is properly dismissed where, as a matter of law, "the allegations in a complaint, however true, could not raise a claim of entitlement to relief." *Twombly*, 550 U.S. at 558. When resolving a motion to dismiss, the Court must assume all well-pleaded facts to be true, "drawing all reasonable inferences in favor of the plaintiff." *See Koch*, 699 F.3d at 145. Pleadings that merely offer "labels and conclusions" or "a formulaic recitation of the elements of a cause of action will not do." *Twombly*, 550 U.S. at 555.

The CFAA, a federal criminal statute, applies to a person who "intentionally accesses a computer without authorization or exceeds authorized access" and obtains information from that unauthorized access. 18 U.S.C. § 1030(a)(2)). Relevant here, the statute provides for a private, civil cause of action in limited circumstances. *See Hancock v. Cnty. of Rensselaer*, 882 F.3d 58, 63 (2d Cir. 2018) ("The scope of the civil actions permitted under [the CFAA] has always been limited"). To state a viable civil claim under the CFAA, CreatorIQ must allege that Staveley (1) intentionally accessed a "protected computer," (2) "without authorization or exceeding

authorized access,” and, relevant here,<sup>6</sup> (3) caused a “loss” of more than \$5,000. *Better Holdco., Inc. v Beeline Loans, Inc.*, No. 20 Civ. 8686 (JPC), 2021 WL 3173736, at \*3 (S.D.N.Y. July 26, 2021).

Defendants move to dismiss the FAC’s CFAA claim on the ground that it does not adequately plead covered loss. Defendants are correct.

The CFAA defines “loss” as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11). To be cognizable, the plaintiff’s “loss” thus must have arisen from identifying and remedying “damage” to the affected computer system. *See El Omari v. Buchanan*, No 20 Civ. 2601 (VM), 2021 WL 5889341, at \*14 (S.D.N.Y. Dec. 10, 2021); *Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 478 (S.D.N.Y. 2004), *aff’d*, 166 F. App’x 559 (2d Cir. 2006).

The CFAA defines “damage,” in turn, as “impairment” of the functioning of the “target computer itself,” *El Omari*, 2021 WL 5889341, at \*14–15; 18 U.S.C. § 1030(e)(8), as opposed to the harm that may have occurred because an unauthorized user obtains or extracts data from the system. *See, e.g., Garland-Sash v. Lewis*, No. 05 Civ. 6827 (WHP), 2011 WL 6188712, at \*3 (S.D.N.Y. Dec. 6, 2011) (“‘[D]amage’ or ‘loss’ under CFAA are inextricably intertwined with a harm to the computer system itself, its data, or delivery of service.”); *Van Buren v. United States*, 593 U.S. 374, 392 (2021) (interpreting “damage” and “loss” in CFAA to “focus on technological

---

<sup>6</sup> “Under the CFAA, a plaintiff must allege that he or she suffered one of five types of statutorily prescribed injuries.” *El Omari v. Buchanan*, No. 20 Civ. 2601 (VM), 2021 WL 5889341, at \*14 (S.D.N.Y. Dec. 10, 2021). The FAC alleges only the aggregate monetary loss injury.

harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data.”).

The FAC, however, does not allege that the defendants’ unauthorized access harmed the functioning of Hubspot or CreatorIQ’s computer systems. It alleges only that Staveley made an unauthorized account using the Hubspot credentials that CreatorIQ had given him, accessed a CreatorIQ-owned Hubspot account without authorization, and exported CreatorIQ’s confidential information. *See* FAC ¶¶ 54–57, 178–80. These allegations describe competitive injuries to CreatorIQ, but not the technological injuries relevant under the CFAA. The FAC does not plead that Staveley harmed the integrity or functioning of the Hubspot system when he accessed or exported CreatorIQ’s files. It does not plead harm to CreatorIQ’s computer systems or to third-party cloud storage. *See Reis, Inc. v. Spring11 LLC*, 15 Civ. 2836 (PGG), 2016 WL 5390896, at \*9 (S.D.N.Y. Sept. 26, 2019) (“Because [defendant] used the [plaintiff’s] Database in exactly the same manner that an authorized user would—by accessing the database via an official username and password—Plaintiffs’ investigation focused not on damage to [plaintiff’s] systems, but rather on identif[ying] . . . [unauthorized] user[s].”); *Deutsch v. Hum. Res. Mgmt.*, 19 Civ. 5305 (VEC), 2020 WL 1877671, at \*5 (S.D.N.Y. Apr. 15, 2020) (dismissing CFAA claims where complaint did not allege any impairment of the protected device and thus did not plead statutory “damage”); *New London Assocs., LLC v. Kinetic Social LLC*, 384 F. Supp. 3d 392, 412 (S.D.N.Y. 2019) (complaint failed to plead damage within CFAA where it did not allege that conduct caused technological inoperability or interruption in service).

CreatorIQ proposes to satisfy the loss element of the CFAA’s loss prong by establishing the cost of the forensic investigation it launched after Staveley’s alleged misconduct. *See* FAC ¶¶ 183–85; *see also* Pl. Br. at 19–21. As pled, however, those costs are not cognizable. The

CFAA's loss element can be met by investigative expenses only to the extent that these arise concerning underlying damage to the computer system itself. Out of bounds are costs of assessing competitive damage to the plaintiff from the misappropriation of its data or from identifying the malefactor behind the unauthorized access. *See Reis, Inc.*, 2016 WL 5390896, at \*9 ("Courts award costs of investigating and repairing the damage, which involves only assessing the damage to the system." (cleaned up)); *cf. Van Buren*, 593 U.S. at 391–92 (statutory definitions of "damage" and "loss" in CFAA focus specifically on technological harms, and are "ill fitted" to "remediating 'misuse' of sensitive information"). Accordingly, "[c]osts associated with locating and collecting information about the hacker are not recoverable under the CFAA." *Reis, Inc.*, 2016 WL 5390896, at \*9.

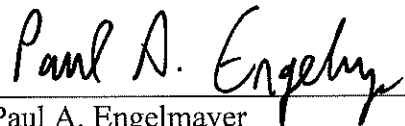
The FAC does not allege investigative costs of this nature. And CreatorIQ's defense of this claim does not describe cognizable costs, either. *See* Pl. Br. at 21 ("Defendants' conduct necessitated an investigation, which included an assessment of not only who accessed CreatorIQ's Hubspot account without authorization, but what was viewed or otherwise misappropriated, and how that unauthorized access was accomplished."). The bare reference to an investigation, absent allegations that the investigation concerned or uncovered damage to the computer system itself, does not plead a viable CFAA claim. *See, e.g., El Omari*, 2021 WL 5889341, at \*14 (dismissing CFAA claim where complaint alleged only costs from efforts to identify the source of an unauthorized access); *Better Holdco*, 2021 WL 3173736, at \*4 (dismissing CFAA claim where complaint alleged only that defendant downloaded and copied data; court notes that an investigation "into the extent of any *misappropriation* of confidential information is not a 'cost of responding to an offense'" (internal quotation marks omitted)).

### CONCLUSION

For the foregoing reasons, the Court grants defendants' motion to dismiss the FAC's claim under the CFAA, and treats the balance of the motion to dismiss as withdrawn.

By separate order, the Court will schedule an initial pre-trial conference. The Clerk of Court is respectfully directed to terminate all pending motions.

SO ORDERED.

  
Paul A. Engelmayer  
United States District Judge

Dated: April 9, 2024  
New York, New York